Begin → initiate a RADIUS session between the user and the network device

100

→ receive a user profile for the user from an AAA server, the user profile containing information regarding which commands the user is authorized to execute

102

→ store the user profile in a cache

104

↓

authorize or reject the command based on the results of the determining

110

← determine whether the command is authorized based on the information in the user profile for the user stored in the cache

108

← receive the command from the user

106

↓

purge the user profile from the cache → End

112

FIG. 1

200
202

oper1   Password = "abc^123"

Service-Type = Login

204   ⌐ Cisco: AVPair = "shell:cmd-expr=show .*",

206   ⌐Cisco: AVPair = "shell:cmd-expr=telnet 10\.14\.0\.[0-9]+",

208   ⌐Cisco: AVPair = "shell:cmd-expr=ping .*"
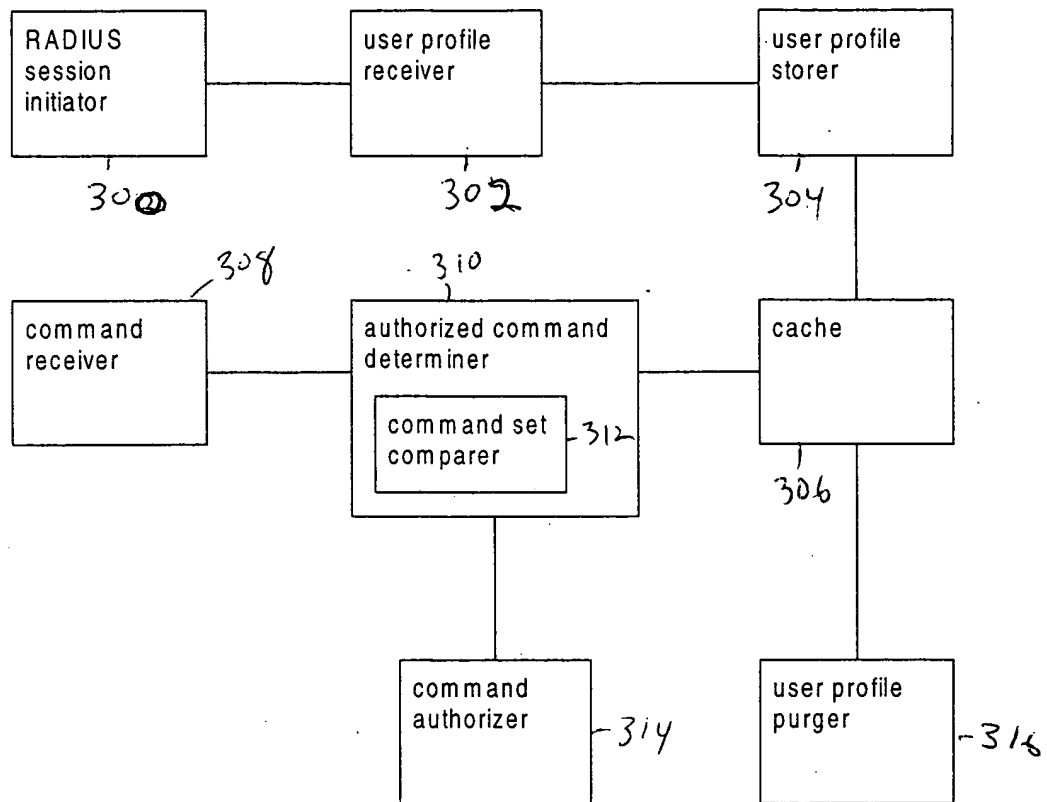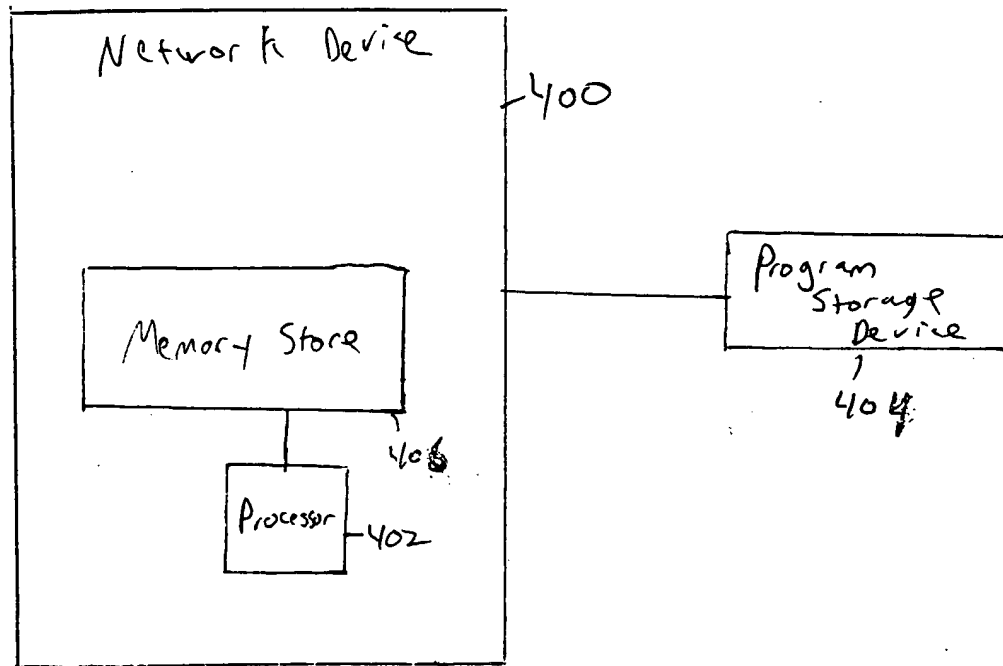
FIG. 2

```
┌──────────────┐     ┌──────────────┐     ┌──────────────┐
│ RADIUS       │     │ user profile │     │ user profile │
│ session      │─────│ receiver     │─────│ storer       │
│ initiator    │     │              │     │              │
└──────────────┘     └──────────────┘     └──────────────┘
      300                  302                  304

┌──────────────┐     ┌──────────────────────┐     ┌──────────────┐
│ command      │     │ authorized command   │     │ cache        │
│ receiver     │─────│ determiner           │─────│              │
│              │     │                      │     │              │
│              │     │ ┌──────────────────┐ │     │              │
│              │     │ │ command set      │ │     └──────────────┘
│              │     │ │ comparer    312  │ │          306
│              │     │ └──────────────────┘ │
└──────────────┘     └──────────────────────┘
      308                     310

                     ┌──────────────┐            ┌──────────────┐
                     │ command      │            │ user profile │
                     │ authorizer   │ 314        │ purger       │ 316
                     │              │            │              │
                     └──────────────┘            └──────────────┘
```

FIG. 3

Network Device

400

Memory Store

Program
Storage
Device

404

406

Processor — 402

FIG. 4